September 2, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cybersecurity Rollup

Included in this week's summary:

Click on the Section Header to go directly to that location in the Summary

NORTH DAKOTA & REGIONAL

(U) Dakota Carrier Network launches statewide Wi-Fi network

(U) Dakota Carrier Network, a provider of broadband and other internet-related services to customers throughout North Dakota, along with its 15 owner companies, announced Aug. 16 it is launching a Wi-Fi network that will allow customers to access DCN's secure network throughout the state.

Source: (U) http://www.prairiebusinessmagazine.com/business/technology/4095658-dakota-carrier-network-launches-statewide-wi-fi-network

NATIONAL

(U) Hotels in Pasadena, San Diego among those hit in data breach

(U) An undisclosed number of people who used credit cards at 20 Hyatt, Sheraton, Marriott, Westin and other hotels in California, nine other states and the District of Columbia may have had their cards compromised as a result of hack of the hotels' payment system.

Source: (U) http://www.latimes.com/business/

INTERNATIONAL

(U) Locky ransomware reverts to malicious macros

(U) FireEye researchers discovered that the Locky ransomware reverted to using Microsoft Office documents embedded with malicious macros to distribute the malware to individuals and organizations in the health care, telecommunications, and transportations industries. Researchers reported that the DOCM files install the ransomware onto a victim's device once the malicious macros are enabled.

Source: (U) http://www.securityweek.com/locky-ransomware-reverts-malicious-macros

(U) Global phishing numbers rise as hosting firms fail to respond

(U) Cyren released its Cyberthreat Report that analyzed global phishing operations and found that the total number of malicious phishing Universal Resource Locators (URLs) spread on the Internet increased by 14 percent in quarter 2 of 2016 to 4.44 million, and revealed that 20 percent of all phishing pages disappear after 3 hours, with only 40 percent of all pages lasting more than 2 days. The report also states that Google Chrome and Mozilla Firefox are the quickest to identify phishing pages and malicious sites after Chrome detected 73.9 percent of phishing pages within 48 hours and Firefox marked 52.2 percent of the sites.

Source: (U) http://news.softpedia.com/news/global-phishing-numbers-rise-as-hostingfirms-fail-to-respond-507441.shtml

(U) Internet Traffic Hijacking Linux Flaw Affects 80% of Android Devices

(U) An estimated 80 percent of Android smartphones and tablets running Android 4.4 KitKat and higher are vulnerable to a recently disclosed Linux kernel flaw that allows hackers to terminate connections, spy on unencrypted traffic or inject malware into the parties' communications. Even the latest Android Nougat Preview is considered to be vulnerable.

Source: (U) http://thehackernews.com/2016/08/hack-linux-android.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1303.iv0ao09bj9.rde

(U) China Launches World's 1st 'Hack-Proof' Quantum Communication Satellite

(U) The satellite, dubbed Quantum Science Satellite, is designed to develop a 'Hack-Proof' communications system in this age of global electronic surveillance and cyber attacks by transmitting uncrackable encryption keys from space to the ground. The 600-plus-kilogram Quantum Science Satellite, better known as Quantum Experiments at Space Scale (QUESS) satellite, took off from the Jiuquan Satellite Launch Center in Gobi Desert at 1:40 AM local time on a 2-year mission on Tuesday.

Source: (U) http://thehackernews.com/2016/08/quantum-communication-satellite.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1303.iv0ao09bj9.rdk

(U) User data leaked from analytics company Social Blade

(U) Social Blade, a data provider for YouTube, Twitch, and Instagram accounts, confirmed that its Website and forum were hacked in August after LeakedSource researchers discovered that the details of 13,009 of the forum's users and 273,806 of the Website's users' details were leaked, including email addresses, usernames, password hashes, and Internet Protocol (IP) addresses, among other information, after a malicious actor obtained a partial database dump by exploiting a vulnerability in the forum software. Social Blade reset all user passwords and shut down its forum.

Source: (U) http://www.securityweek.com/user-data-leaked-analytics-company-socialblade

(U) Apple releases 'Emergency' Patch after Advanced Spyware Targets Human Rights Activist

(U) Apple has released iOS 9.3.5 update for iPhones and iPads to patch three zero-day vulnerabilities after a piece of spyware found targeting the iPhone used by a renowned UAE human rights defender, Ahmed Mansoor.

Source: (U) http://thehackernews.com/2016/08/apple-security-update.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1309.iv0ao09bj9.rik